(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 August 2005 (25.08.2005)

PCT

(10) International Publication Number
WO 2005/078988 A1

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number:
PCT/SE2004/000179

(22) International Filing Date: 11 February 2004 (11.02.2004)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **BLOM, Rolf** [SE/SE]; Svärdvägen 2, S-175 68 Järfalla (SE). **NÄSLUND, Mats** [SE/SE]; Grimstagatan 161, S-162 58 Vällingby (SE). **CARRARA, Elisabetta** [SE/SE]; Malmvägen 6B, S-19161 Sollentuna (SE). **LINDHOLM, Fredrik** [SE/SE]; Stamgatan 87, S-125 74 Älvsjö (SE). **NORRMAN, Karl** [SE/SE]; Bondegatan 3B, S-116 23 Stockholm (SE).

(74) Agent: **AROS PATENT AB**; P.O. Box 1544, S-751 45 Uppsala (SE).

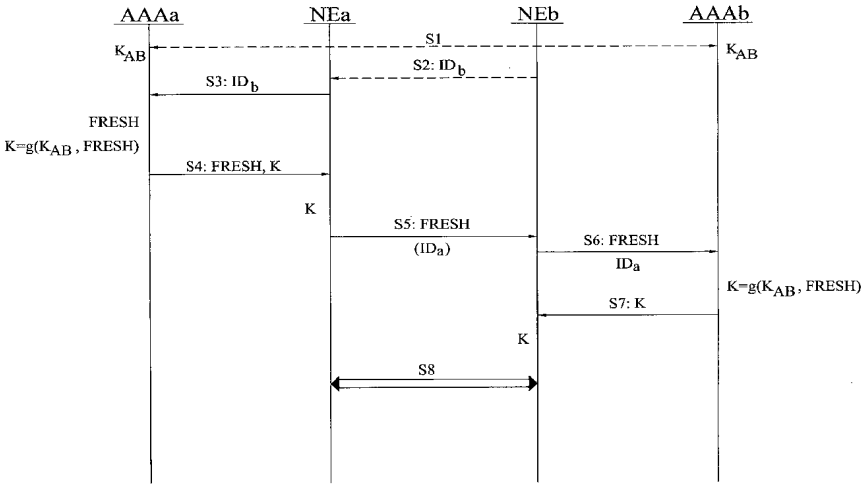
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

[Continued on next page]

(54) Title: KEY MANAGEMENT FOR NETWORK ELEMENTS



(57) Abstract: The invention provides an establishment of a secret session key shared Between two network elements (NEa, NEb) belonging to different network domains (NDa, NDb). A first network element (NEa) of a first network domain (NDa) requests security parameters from an associated key management center (KMC) (AAAa). Upon reception of the request, the KMC (AAAa) generates a freshness token (FRESH) and calculates the session key (K) based on this token (FRESH) and a master key (KAB) shared with a second network domain (NDb). The security parameters are (securely) provided to the network element (NEa), which extracts the session key (K) and forwards the freshness token (FRESH) to the KMC (AAAb) of the second domain (NDb) through a second network element (NEb). Based on the token (FRESH) and the shared master key (KAB), the KMC (AAAb) generates a copy of the session key (K), which is (securely) provided to the second network element (NEb). The two network elements (NEa, NEb) now have shares the session key (K), enabling them to securely communicate with each other.

WO 2005/078988 A1

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.